IT2018 EHK-EHTOJEN KÄYTTÖ

Henkilötietojen käsittely (EHK)

Henkilötietojen käsittelyä koskevien EHK-ehtojen taustalla on EU:n tietosuoja-asetus (679/2016). Sen mukaan henkilötietojen käsittelystä on sovittava kirjallisin sopimuksin, kun henkilötietojen käsittelijä käsittelee henkilötietoja rekisterinpitäjän lukuun.

EHK-ehdot on tarkoitettu käytettäväksi yhdessä yleisten sopimusehtojen (YSE) kanssa silloin, kun toimittaja käsittelee henkilötietoja asiakkaan lukuun. Tällöin asiakas on tietosuoja-asetuksen mukainen rekisterinpitäjä ja toimittaja on henkilötietojen käsittelijä.

EHK-ehtojen tarkoitus on varmistaa, että osapuolet sopivat kirjallisesti niistä seikoista, joista henkilötietojen käsittelyä koskevassa sopimuksessa on tietosuoja-asetuksen mukaan sovittava. Osasta EHK-ehtojen yksityiskohdista voidaan sopia toisinkin, mutta koska osapuolten liikkumavaraa rajoittavat erityisesti tietosuoja-asetuksen 28 artiklan pakottavat normit, ne tulee tarkastaa aina ennen EHK-ehtojen sanamuodoista poikkeamista. Samasta syystä IT2018-ehtoja laadittaessa lähtökohtana on ollut se, että EHK-ehdot ovat soveltamisjärjestyksessä ensisijainen suhteessa muihin IT2018-erityisehtoihin ja YSE-ehtoihin.

EHK-ehdoissa esitetyt määritelmät noudattavat tietosuoja-asetuksen mukaisia määritelmiä, joiden sisältöä kuvataan seuraavassa tarkemmin:

- **Henkilötieto**. Henkilötiedon määritelmä on laaja kattaen kaikki *tunnistettuun tai tunnistettavissa olevaan* luonnolliseen henkilöön (rekisteröity) liittyvät tiedot. Tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan *suoraan tai epäsuorasti* tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen (esim. eväste) taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella. Henkilötietoja ovat esimerkiksi nimi, henkilötunnus, kuva, henkilön yksilöivä sähköpostiosoite tai puhelinnumero tai asiakasnumero. Oikeuskäytännössä on katsottu, että myös IP-osoite voi olla henkilötieto.

  Tietosuoja-asetuksen mukaan myös pseudonymisoitu tieto on henkilötieto. Pseudonymisoinnilla tarkoitetaan sitä, että henkilötietoja ei voida enää yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja. Pseudonyyminkin tiedon käsittelyyn soveltuu tietosuoja-asetus ja siten henkilötietojen käsittelyä koskevan sopimuksen laatimisvelvollisuus. Ainoastaan silloin, kun tietojen tunnistettavuus on poistettu lopullisesti siten, ettei rekisteröidyn suora tai epäsuora tunnistaminen ole enää mahdollista omassa tai toisen hallussa olevia lisätietoja käyttämälläkään, tietosuoja-asetus ei sovellu (esim. tilastotieto).

  Yritykseen liittyvät tiedot eivät ole henkilötietoja. Kun tieto kuitenkin liittyy yksittäiseen luonnolliseen henkilöön, on kysymys henkilötiedosta (esim. yhtiön edustajan nimi).

ISBN 978-952-238-223-8
www.it-ehdot.fi

- **Käsittely**. Myös henkilötietojen käsittelyn määritelmä on erittäin laaja. Käsittely tarkoittaa kaikkia toimintoja, joita henkilötietojen käsittelijä (toimittaja) tekee rekisterinpitäjän (asiakas) lukuun sopijapuolten välisen sopimuksen perusteella ja joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista. Jo pelkkä henkilötietojen säilyttäminen asiakkaan lukuun toimittajan palvelimella on henkilötietojen käsittelyä.

- **Rekisterinpitäjä**. Rekisterinpitäjä on luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen *käsittelyn tarkoitukset ja keinot*.

- **Henkilötietojen käsittelijä**. Käsittelijällä tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Kyse voi olla esimerkiksi toimeksianto- tai alihankintasuhteesta, jossa yritys (rekisterinpitäjä) ulkoistaa asiakastietojensa säilytyksen pilvipalveluun, jolloin pilvipalveluntarjoaja toimii henkilötietojen käsittelijänä.

Joissakin tilanteissa voi olla niin, että sopimuksen molemmat osapuolet toimivat osin rekisterinpitäjinä ja osin käsittelijöinä (joskin keskenään eri käsittelytarkoituksissa), tai yhteisrekisterinpitäjinä. Tällaisiin erityistilanteisiin EHK-ehdot eivät sovellu sellaisinaan, vaan niitä on muutettava soveltuvin osin kattamaan poikkeava käsittelytilanne.

Sopimusta tehtäessä sopijapuolten tulisi kiinnittää huomiota erityisesti seuraaviin ehtoihin ja niiden taustalla oleviin tietosuoja-asetuksen mukaisiin vaatimuksiin:

EHK 3: Yleiset oikeudet ja velvollisuudet henkilötietojen käsittelyssä

Henkilötietojen käsittelyssä on olennaista käyttötarkoitussidonnaisuus: henkilötietoja saa tietosuoja-asetuksen mukaan kerätä ja käsitellä vain tiettyä, nimenomaista ja laillista tarkoitusta varten. Tämän tarkoituksen ja käsittelyn keinot määrittelee rekisterinpitäjä (asiakas). Käsittelijä (toimittaja) ei saa käyttää tietoja muihin käyttötarkoituksiin, eikä luovuttaa ilman lupaa henkilötietoja kolmansille näiden omiin käyttötarkoituksiin.

Käyttötarkoitus on aina tapauskohtaista, ja se on erikseen määriteltävä osapuolten välisessä sopimuksessa. Henkilötietojen käsittelysopimuksessa on sovittava seuraavista pakollisista henkilötietojen käsittelyn yksityiskohdista: (a) henkilötietojen käsittelyn kohde ja kesto, (b) henkilötietojen käsittelyn luonne ja tarkoitus, (c) henkilötietojen tyyppi ja rekisteröityjen ryhmät ja (d) soveltuvat tietoturvatoimenpiteet.

Tietosuoja-asetus asettaa käsittelijälle tiedonantovelvollisuuksia, mukaan lukien velvollisuus antaa rekisterinpitäjälle tietoja, joita tämä voi tarvita (i) toteuttaakseen rekisteröityjen tietosuoja-asetuksen mukaiset oikeudet (kuten esimerkiksi tarkastus-, korjaus-, poisto- ja tietojen siirto-oikeudet) tai (ii) noudattaakseen tietosuojaviranomaisten vaatimuksia tai ohjeistusta. EHK-ehdoissa lähtökohtana on, että

ISBN 978-952-238-223-8
www.it-ehdot.fi

toimittajalla on oikeus veloittaa asiakasta näistä toimenpiteistä yleisen hinnastonsa mukaisesti, elleivät osapuolet toisin sovi.

EHK 4: Auditoinnit

Tietosuoja-asetuksen mukaan käsittelijän on tiedonantovelvollisuuksiensa lisäksi sallittava rekisterinpitäjän tai muun rekisterinpitäjän valtuuttaman auditoijan suorittamat auditoinnit.

Silloin, kun henkilötietojen käsittelijä (toimittaja) käyttää toisen henkilötietojen käsittelijän (alihankkija) palveluksia henkilötietojen käsittelytoimintojen suorittamiseksi rekisterinpitäjän (asiakas) puolesta, alihankkijaan sovelletaan samoja tietosuojavelvoitteita kuin ne, jotka on vahvistettu toimittajan ja asiakkaan välisessä sopimuksessa.

EHK 5: Tietoturva

Yleinen tietoturva

Rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi niin, että käsittely täyttää tietosuoja-asetuksen vaatimukset ja sillä varmistetaan rekisteröidyn oikeuksien suojelu. Käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet, ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit.

Asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota etenkin käsittelyn sisältämiin riskeihin, erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi.

Henkilötietojen käsittelijän tulee myös varmistaa, että henkilöt, joilla on oikeus käsitellä henkilötietoja, ovat sitoutuneet noudattamaan salassapitovelvollisuutta tai heitä koskee asianmukainen lakisääteinen salassapitovelvollisuus.

EHK-ehtojen liitteeksi tulevassa asiakirjassa (ks. EHK-ehtojen kohtaa 3 koskevat kommentit edellä) voidaan täsmentää osapuolten kesken sitä, mitä tietoturvatoimenpiteitä toimittajalta edellytetään.

Tietoturvaloukkaukset

Rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta toimivaltaiselle valvontaviranomaiselle, paitsi jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Tietoturvaloukkauksesta tulee ilmoittaa myös rekisteröidylle, kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille.

Tietosuoja-asetuksen mukaan käsittelijän on avustettava rekisterinpitäjää varmistamaan myös näiden tietosuojarikkomuksia koskevien artiklojen noudattaminen. Tästä syystä EHK-ehtojen 5 kohtaan on

ISBN 978-952-238-223-8
www.it-ehdot.fi

kirjattu soveltuvin osin käsittelijän vastuista tiedottaa tietoturvaloukkauksista tavalla, jotka mahdollistavat rekisterinpitäjän toteuttamaan omat tiedonantovelvollisuutensa tietosuoja-asetuksen mukaisissa määräajoissa.

EHK 6: Henkilötietojen sijainti

Tietosuoja-asetuksen mukaan henkilötietojen siirto EU:n/ETA-alueen ulkopuolelle on lähtökohtaisesti kiellettyä, jollei tietosuoja-asetuksen mukaisia siirtomekanismeja ole otettu käyttöön.

- **Henkilötietojen siirtona** pidetään tietosuoja-asetuksen nojalla tietojen fyysisen siirtämisen ja lähettämisen lisäksi myös esimerkiksi sitä, että EU:n/ETA-alueen ulkopuoliselle vastaanottajalle annetaan pääsy EU:ssa sijaitsevan rekisterinpitäjän tietokantaan ja sitä, että henkilötietoja julkaistaan internetissä. Siirtäminen EU:n/ETA-alueen ulkopuolelle ei edellytä siirtoa kolmannelle taholle, vaan henkilötietojen siirtoa koskeva sääntely soveltuu silloinkin, kun tiedot siirretään käsittelijän omalle palvelimelle EU:n/ETA-alueen ulkopuolelle.

EHK-ehdoissa lähtökohdaksi on otettu se, että käsittelijällä on oikeus siirtää henkilötietoja palvelun toteuttamista varten EU:n/ETA-alueen ulkopuolelle (esim. EU:n/ETA-alueen ulkopuolella olevalle palvelimelle), ellei toisin ole sovittu. Tällöin käsittelijän on huolehdittava siitä, että siirto toteutetaan tietosuoja-asetuksen mukaisia menettelytapoja noudattaen, esimerkiksi (a) varmistuen, että kohdevaltio on maa, jonka osalta Euroopan komissio on päättänyt kyseisen maan takaavan henkilötiedoille riittävän tietosuojan tason, (b) käyttäen komission kulloinkin hyväksymiä mallisopimuslausekkeita ("*standard contractual clauses*"), (c) yritystä koskevien, tietosuojaviranomaisen vahvistamien sitovien sääntöjen nojalla ("*binding corporate rules*") tai (d) ns. Privacy Shield -sertifioinnin perusteella, jos kysymys on siirrosta sertifioinnin piiriin kuuluvalle yhdysvaltalaiselle yritykselle.

EHK-ehtojen kohdan 6.1 mukaisesti asiakkaalla on milloin tahansa oikeus saada toimittajalta tiedot henkilötietojen käsittelyn sijainnista voidakseen täyttää omat tietosuoja-asetuksen mukaiset tiedonanto- ja osoitusvelvollisuutensa rekisterinpitäjänä.

EHK 7: Kolmansien osapuolten käyttäminen henkilötietojen käsittelyssä

Henkilötietojen käsittelijä ei saa käyttää toisen henkilötietojen käsittelijän palveluksia (alihankkija) ilman rekisterinpitäjän erityistä tai yleistä kirjallista ennakkolupaa. EHK-ohjeiden kohtaan 7 on kirjattu tällainen yleinen ennakkolupa, mutta halutessaan osapuolet voivat sopia tapauskohtaisesti ennakkoluvan pyytämisvelvollisuudesta.

Kun henkilötietojen käsittelijä käyttää alihankkijaa henkilötietojen käsittelemiseksi rekisterinpitäjän puolesta, kyseiseen toiseen henkilötietojen käsittelijään sovelletaan sopimuksen mukaisesti samoja tietosuojavelvoitteita kuin ne, jotka on vahvistettu rekisterinpitäjän ja henkilötietojen käsittelijän välisessä sopimuksessa. Tästä syystä toimittajan on huolehdittava samojen ehtojen sisällyttämisestä sopimukseensa alihankkijan kanssa, ml. esimerkiksi tietoturvavelvoitteet ja asiakkaan auditointioikeudet.

Tietosuoja-asetuksen mukaan kirjallisen ennakkoluvan tilanteessa henkilötietojen käsittelijän on tiedotettava rekisterinpitäjälle kaikista suunnitelluista muutoksista, jotka koskevat muiden henkilötietojen käsittelijöiden lisäämistä tai vaihtamista, ja annettava siten rekisterinpitäjälle mahdollisuus vastustaa

ISBN 978-952-238-223-8
www.it-ehdot.fi

tällaisia muutoksia. EHK-ehtoihin on kirjattu menettelytavat vastustamisoikeuden käytölle, mutta menettelytavoista voidaan sopia toisinkin tietosuoja-asetuksen asettamissa rajoissa.

Kun henkilötietojen käsittelijän (toimittaja) käyttämä toinen henkilötietojen käsittelijä (alihankkija) ei täytä tietosuojavelvoitteitaan, alkuperäinen henkilötietojen käsittelijä on tietosuoja-asetuksen mukaan edelleen täysimääräisesti vastuussa toisen henkilötietojen käsittelijän velvoitteiden suorittamisesta suhteessa rekisterinpitäjään. EHK-ehtojen 7.4 kohta vastaa tätä ja on yhdenmukainen YSE-ehtojen kohdan 6 periaatteen kanssa, jonka mukaan toimittaja vastaa alihankkijan toiminnasta kuin omastaan.

EHK 8: Henkilötietojen poistaminen ja palauttaminen

EHK-ehtojen 8.2 kohta peilaa tietosuoja-asetuksen mukaista vaatimusta noudattaa rekisterinpitäjän ohjeita henkilötietojen käsittelyssä, ml. henkilötietojen poistaminen. Osapuolten välisessä kirjallisessa sopimuksessa on sovittava siitä, että käsittelijä rekisterinpitäjän valinnan mukaan poistaa tai palauttaa käsittelyyn liittyvien palveluiden tarjoamisen päätyttyä kaikki henkilötiedot rekisterinpitäjälle ja poistaa olemassa olevat jäljennökset. Kohtaan 8.2 on myös kirjattu menettelytapa, jota noudatetaan silloin, kun rekisterinpitäjä ei anna erityisiä ohjeita poistamisesta tai palauttamisesta.

EHK 9: Korvausvelvollisuus ja vastuunrajoitukset

Sopijapuolet voivat sopia korvausvelvollisuudesta ja vastuunrajoituksista tapauskohtaisesti. Elleivät sopijapuolet näin tee, sovelletaan IT2018 YSE yleisten sopimusehtojen kohtaa 13 siten, että YSE-ehtojen kohdan 13.2 mukainen sopijapuolen vahingonkorvausvelvollisuuden enimmäismäärä on kaksinkertainen verrattuna YSE-ehtojen kohdassa 13.2 sovittuun.

ISBN 978-952-238-223-8
www.it-ehdot.fi